

Totally symmetric dessins with nilpotent automorphism groups of class three

Na-Er Wang^{*1,2}, Roman Nedela^{†3,4}, and Kan Hu^{‡1,2}

¹School of Mathematics, Physics and Information Science,
Zhejiang Ocean University, Zhoushan, Zhejiang 316022, People's
Republic of China

²Key Laboratory of Oceanographic Big Data Mining &
Application of Zhejiang Province, Zhoushan, Zhejiang 316022,
People's Republic of China

³Faculty of Natural Sciences, Matej Bel University, Tajovského
40, 974 01, Banská Bystrica, Slovak Republic

⁴Institute of Mathematics and Computer Science, Slovak
Academy of Sciences, Banská Bystrica, Slovak Republic

November 24, 2015

Abstract

A dessin is a 2-cell embedding of a connected bipartite graph into an orientable closed surface. An automorphism of a dessin is a permutation of the edges of the underlying graph which preserves the colouring of the vertices and extends to an orientation-preserving self-homeomorphism of the supporting surface. A dessin is regular if its automorphism group is transitive on the edges, and a regular dessin is totally symmetric if it is invariant under all dessin operations. Thus totally symmetric dessins possesses the highest level of external symmetry. In this paper we present a classification of totally symmetric dessins with a nilpotent automorphism group of class three.

^{*}wangnaer@zjou.edu.cn

[†]nedela@savbb.sk

[‡]hukan@zjou.edu.cn

Keywords regular dessin, dessin operation, external symmetry.
MSC(2010) Primary 14H57; Secondary 14H37, 20B25, 30F10

1 Introduction

By Belyĭ's theorem [1], a compact Riemann surface S , regarded as an algebraic curve, is definable over the field $\bar{\mathbb{Q}}$ of algebraic numbers if and only if there is a non-constant meromorphic function β from S to the Riemann sphere with at most three critical values. By composing β with a Möbius transformation when necessary, these three critical points can be chosen as $\{0, 1, \infty\}$. Joining 0 and 1 with a single edge we obtain the trivial bipartite map on the Riemann sphere, which lifts along β to a bipartite map on S : The embedded bipartite graph is the preimage $\beta^{-1}[0, 1]$ of the closed interval $[0, 1]$, and the black and the white vertices are the preimages of 0 and 1 respectively.

The absolute Galois group $\mathbf{G} := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ has a natural action on the coefficients of polynomials and rational functions which define the Riemann surfaces and Belyĭ functions. In particular, it induces an action of \mathbf{G} on the bipartite maps. Grothendieck showed that this action is faithful [10], so we have a combinatorial approach to \mathbf{G} . Following Grothendieck such bipartite maps will be called dessins.

A dessin D is regular if the associated Belyĭ function β is a regular covering, in which case the automorphism group $\text{Aut}(D)$ of D , the group of covering transformations of β , acts transitively on the edges of D . Recently, González-Diez and Jaikin-Zapirain have shown that the action of \mathbf{G} on dessins remains faithful when restricted to regular dessins [9].

An important problem in this field is the classification of regular dessins, typically imposing certain conditions on the supporting surfaces, the embedded graphs or the underlying automorphism groups [3, 5, 7, 8, 11, 12, 14, 15, 18, 20].

In this paper we investigate regular dessins with nilpotent automorphism groups, with emphasis on totally symmetric ones, i.e., regular dessins which are invariant under all dessin operations. As shown by Jones in [15], every nilpotent regular dessin is covered by a nilpotent totally symmetric dessin. Totally symmetric dessins with nilpotent automorphism groups of class one and two have been classified in [11, 12]. The main result of the present paper is a classification of totally symmetric dessins with nilpotent automorphism groups of nilpotent class three, see Theorem 15.

2 Algebraic theory of dessins

In this section we outline the algebraic theory of regular dessin and dessin operations. For more details the reader is referred to [16] and [15].

Each dessin D on an orientable surface S determines a two-generator transitive permutation group $\text{Mon}(D) = \langle \rho, \lambda \rangle$ on the edge set E of D : The global orientation of S induces two permutations ρ and λ which cyclically permute the edges incident with each black and each white vertex of D ; since the underlying graph of D is connected, the group $\text{Mon}(D) = \langle \rho, \lambda \rangle$ is transitive. Let

$$F_2 = \langle X, Y \mid - \rangle,$$

i.e., F_2 is the free group of rank two. Then we have a transitive permutation representation of F_2 defined by

$$F_2 \rightarrow \text{Mon}(D), X \mapsto \rho, Y \mapsto \lambda.$$

In this representation the black and the white vertices correspond to the orbits of the subgroups $\langle X \rangle$ and $\langle Y \rangle$, respectively, and the faces correspond to the orbits of $\langle XY \rangle$, with incidence given by non-empty intersection.

The stabilizer $N := \text{Stab}_{F_2}(e)$ in F_2 of an edge e is a subgroup of finite index in F_2 . This subgroup is uniquely determined up to conjugacy. It will be called the *dessin subgroup* associated with D . Moreover, an automorphism σ of F_2 sends N to N^σ , and hence transforms D to a dessin D^σ . In particular if σ is an inner automorphism of F_2 , then N is conjugate to N^σ , and hence D is isomorphic to D^σ . It follows that the outer automorphism group

$$\Omega := \text{Out}(F_2) = \text{Aut}(F_2)/\text{Inn}(F_2)$$

of F_2 acts as the *group of dessin operations* on the isomorphism classes of dessins. It is well known that $\text{Aut}(F_2)$ is generated by the elementary Nielsen transformations of the form

$$\begin{aligned} \tau : X \rightarrow Y, Y \rightarrow X, \quad \pi_1 : X \rightarrow X, Y \rightarrow Y^{-1}, \quad \pi : X \rightarrow X^{-1}, Y \rightarrow Y, \\ \zeta : X \rightarrow XY, Y \rightarrow Y, \quad \eta : X \rightarrow X, Y \rightarrow YX. \end{aligned}$$

This is not a minimal set of generators. For instance we have

Proposition 1. $\text{Aut}(F_2) = \langle \tau, \pi, \zeta \rangle$ and $\Omega = \langle \omega_\tau, \omega_\pi, \omega_\zeta \rangle$ where $\omega_\tau, \omega_\pi, \omega_\zeta$ are dessin operations induced by the automorphisms τ, π, ζ of F_2 .

Proof. Note that $\pi_1 = \tau\pi\tau$ and $\eta = \tau\zeta\tau$, we have $\text{Aut}(F_2) = \langle \tau, \pi, \zeta \rangle$, and hence $\Omega = \langle \omega_\tau, \omega_\pi, \omega_\zeta \rangle$. \square

The operation ω_τ on dessins transposes the black and white vertices while preserves the faces and orientation. The operation ω_π reverses the orientation around the black vertices while preserves it around the white vertices. It is sometimes called the Petrie operation, since it transposes the faces with the Petrie polygons (the zig-zag paths). Finally, let $\iota = \pi\pi_1$, then the operation ω_ι transforms a dessin into its mirror image by reversing the orientation around the black and white vertices.

The most important dessins are regular dessins, in which both $\text{Mon}(D)$ and $\text{Aut}(D)$ are regular permutation groups on E , and the associated dessin subgroups N are normal in F_2 . In particular we have

$$\text{Mon}(D) \cong \text{Aut}(D) \cong F_2/N.$$

In a regular dessin D one may identify D with the underlying set of $G := \text{Aut}(D)$, and the groups $\text{Aut}(D)$ and $\text{Mon}(D)$ with the left and right regular representations of G , respectively. So each regular dessin D gives rise to an *algebraic dessin* – a triple (G, x, y) where x and y generate the stabilizers of a pair of adjacent (black and white) vertices in G , and hence $G = \langle x, y \rangle$.

Moreover, for an automorphism $\sigma \in \text{Aut}(F_2) \setminus \text{Inn}(F_2)$, if the normal subgroup N in F_2 is σ -invariant, i.e., $N = N^\sigma$, then the associated regular dessin D is invariant under the dessin operation ω_σ , i.e., $D \cong D^\sigma$. In this case we say that the regular dessin D possesses the *external symmetry* σ . More specifically, a regular dessin D will be called *symmetric* (resp. *self-Petrie-dual*, *reflexible*) if it is invariant under the operation ω_τ (resp. ω_π , ω_ι). A regular dessin which is invariant under all dessin operations will be called *totally symmetric*. It follows that a regular dessin is totally symmetric if and only if the associated dessin subgroup N is characteristic in F_2 , in which case we have a natural homomorphism $\text{Aut}(F_2) \rightarrow \text{Aut}(G)$ where $G \cong F_2/N$. In particular each of the following assignments extends to an automorphism of G (By abuse of notation we have retained the Greek letters used above):

$$\begin{aligned} \tau : x &\mapsto y, & y &\mapsto x; \\ \pi : x &\mapsto x^{-1}, & y &\mapsto y; \\ \zeta : x &\mapsto xy, & y &\mapsto y. \end{aligned} \tag{1}$$

Define $\iota = \pi\tau\pi\tau$ and $\nu = \iota\tau\zeta\tau\iota$. Then

$$\iota : x \mapsto x^{-1}, \quad y \mapsto y^{-1} \quad \text{and} \quad \nu : x \mapsto x, \quad y \mapsto xy.$$

Lemma 2. *Let (G, x, y) be a totally symmetric dessin, then $\langle y \rangle \cap G' = \langle y \rangle \cap \langle x, G' \rangle$.*

Proof. It suffices to prove that $\langle y \rangle \cap \langle x, G' \rangle \subseteq G'$. Assume that $\langle y \rangle \cap \langle x, G' \rangle = \langle y^{p^m} \rangle$ where m is a nonnegative integer. Then

$$y^{p^m} = x^{rp^n} g_1, \quad (2)$$

where r and n are nonnegative integers, $\gcd(r, p) = 1$, and $g_1 \in G'$. Applying τ to (2) we have

$$x^{p^m} = \tau(y^{p^m}) = \tau(x^{rp^n} g_1) = \tau(x^{rp^n}) \tau(g_1) = y^{rp^n} \tau(g_1). \quad (3)$$

So we have $y^{rp^n} = x^{p^m} \tau(g_1)^{-1} \in \langle x, G' \rangle$. By the minimality of m we have $m \leq n$.

If $m = n$, then applying $\nu = \iota \tau \zeta \tau \iota : x \mapsto x, y \mapsto xy$ to (2) we have

$$(xy)^{p^m} = \nu(y^{p^m}) = \nu(x^{rp^n} g_1) = x^{rp^m} \nu(g_1).$$

By Hall-Petrescu formula [2, Theorem A.1.3] $(xy)^{p^m} = x^{p^m} y^{p^m} g_2$ where $g_2 \in G'$. So $x^{p^m} y^{p^m} g_2 = x^{rp^m} \nu(g_1)$, and hence $x^{(1-r)p^m} y^{p^m} = \nu(g_1) g_2^{-1}$. It follows that

$$x^{p^m} = x^{(1-r)p^m} x^{rp^m} \stackrel{(2)}{=} x^{(1-r)p^m} y^{p^m} g_1^{-1} = \nu(g_1) g_2^{-1} g_1^{-1} \in G'.$$

Therefore $y^{p^m} = \tau(x^{p^m}) = \tau(\nu(g_1) g_2^{-1} g_1^{-1}) \in G'$.

On the other hand, if $m < n$, then by (2) and (3) we have

$$y^{p^m} \stackrel{(2)}{=} x^{rp^n} g_1 = (x^{p^m})^{rp^{n-m}} g_1 \stackrel{(3)}{=} (y^{rp^n} \tau(g_1))^{rp^{n-m}} g_1 = y^{r^2 p^{2n-m}} g_3,$$

where $g_3 \in G'$. So $y^{p^m(1-r^2 p^{2n-2m})} = g_3 \in G'$. Since $\gcd(r, p) = 1$ and $n > m$, we have $\gcd(p, 1 - r^2 p^{2n-2m}) = 1$. Consequently $y^{p^m} \in G'$. \square

Proposition 3. [15] *Let G be a finite two-generator group, then*

- (i) *the set $\mathcal{R}(G)$ of isomorphism classes of regular dessins D with $\text{Aut}(D) \cong G$ corresponds bijectively to the set $\mathcal{N}(G)$ of normal subgroups N of F_2 such that $F_2/N \cong G$.*
- (ii) *The isomorphism classes of regular dessins D with $\text{Aut}(D) \cong G$ are in one-to-one correspondence with the orbits of the action of $\text{Aut}(G)$ on the generating pairs of G .*

Note that the number $|\mathcal{R}(G)| = |\mathcal{N}(G)|$ is finite. Define

$$K(G) = \bigcap_{N \in \mathcal{N}(G)} N.$$

Then $K(G)$, being the intersection of finitely many normal subgroups of finite index in F_2 , is normal of finite index in F_2 . Let $U(G)$ be the regular dessin associated with $K(G)$, and $\bar{G} = F_2/K(G)$. Then $U(G)$ is the smallest regular dessin which covers all regular dessins in $\mathcal{R}(G)$. The construction of $U(G)$ and \bar{G} implies that $U(G)$ is the *unique* regular dessin with an automorphism group isomorphic to \bar{G} . The uniqueness implies that $U(G)$ is totally symmetric, and is defined over the field of rational numbers. In particular, if G is nilpotent of class c , then so is \bar{G} [15].

Example 4. [15, Example 5.1] Let m, n be positive integers, and $m \mid n$. If $G \cong C_n \times C_m$, the direct product of two cyclic groups of orders n and m , then $\bar{G} \cong C_n \times C_n$, and $U(G)$ is the n th degree Fermat dessin, corresponding to the standard embedding of $K_{n,n}$ [14] into the Fermat curve

$$x_0^n + x_1^n + x_2^n = 0.$$

in $\mathbb{P}^2(\mathbb{C})$.

For a regular dessin $D = (G, x, y)$, the type of D is the triple (l, m, n) where

$$l = o(x), \quad m = o(y), \quad n = o(xy),$$

the orders of the elements x, y and xy . It has genus g determined by the Euler-Poincaré formula:

$$2 - 2g = |G| \left(\frac{1}{l} + \frac{1}{m} + \frac{1}{n} - 1 \right).$$

3 Nilpotent groups

In this section, we summarise some preliminary results on nilpotent groups to be used later.

Let G be a group, the commutators of order n are defined recursively by the rule

$$[x_1, x_2] = x_1^{-1}x_2^{-1}x_1x_2, \quad [x_1, x_2, \dots, x_n] = [[x_1, x_2, \dots, x_{n-1}], x_n], \quad n > 2$$

where $x_i \in G$. For subgroups H, K of G , the notation $[H, K]$ will mean the group generated by all $[x, y]$ with $x \in H$ and $y \in K$. In particular, $[G, G]$ is the commutator subgroup of G . We define recursively the n th derived subgroup of G by the rule

$$G' = G^{(1)} = [G, G], \quad G'' = G^{(2)} = [G', G'], \quad G^{(n)} = [G^{(n-1)}, G^{(n-1)}], \quad n \geq 3.$$

A group is solvable if the sequence

$$G \geq G' \geq G'' \geq \dots$$

terminates at the identity group in a finite number of steps, say $G^{(d)} = 1$. The number d is the derived length of G . In particular, G is called *metabelian* if $G'' = 1$. Moreover, the *lower central series* of G is

$$G = G_1 \geq G_2 \geq G_3 \geq \dots$$

where $G_2 = [G, G]$ and $G_i = [G_{i-1}, G]$ ($i \geq 3$), and the *upper central series* of G is

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

where $Z_1(G) = Z(G)$, the center of G , and $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$ ($i \geq 2$). A group is *nilpotent* if its lower central series terminates at the identity group in a finite number of steps. This is equivalent to that its upper central series contains G in a finite steps [13]. If G is a nilpotent, then its upper central series and lower central series have finite length and both have the same length c . The number c is called the class of G . In general if G is nilpotent of class c , then for each j ($0 \leq j \leq c$), $G_{c+1-j} \leq Z_j(G)$ [23, Lemma 1.7.9]. So if $c = 3$ and $j = 0$, then $G_4 \leq Z_0(G) = 1$. Since $G^{(i)} \leq G_{2^i}$ [13, Theorem III.2.12], we have $G'' = 1$. That is, G is a metabelian group.

Lemma 5. [23, Proposition 2.1.5] Let G be a metabelian group, $x_i \in G$ ($i = 1, 2, \dots, n$). If $z \in G'$, then

$$[z, x_1, x_2, \dots, x_n] = [z, x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}].$$

where α is an arbitrary permutation of $\{1, 2, \dots, n\}$.

By Lemma 5, for brevity, we may define

$$[ix, jy] = [x, y, \underbrace{x, \dots, x}_{i-1}, \underbrace{y, \dots, y}_{j-1}].$$

where i and j are positive integers.

Lemma 6. [23, Proposition 2.1.6] Let G be a metabelian group generated by x and y . Then for any $s \geq 2$,

$$G_s = \langle [ix, (s-i)y], G_{s+1} \mid i = 1, 2, \dots, s-1 \rangle.$$

Lemma 7. [23, Proposition 2.1.7] Let G be a metabelian group, $x, y \in G$. Then for any positive integers m and n

$$[x^m, y^n] = \prod_{i=1}^m \prod_{j=1}^n [ix, jy]^{\binom{m}{i} \binom{n}{j}}. \quad (4)$$

Lemma 8. [23, Proposition 2.1.8] Let G be a metabelian group, $x, y \in G$. Then for any integer $m \geq 2$

$$(xy^{-1})^m = x^m \left(\prod_{i+j \leq m} [ix, jy]^{\binom{m}{i+j}} \right) y^{-m}. \quad (5)$$

Corollary 9. Let G be a nilpotent group of class 3, $x, y \in G$. Then for any nonnegative integers m and n ,

$$\begin{aligned} [x^m, y^n] &= [x, y]^{mn} [x, y, x]^n \binom{m}{2} [x, y, y]^m \binom{n}{2}, \\ (xy^{-1})^m &= x^m y^{-m} [x, y]^{\binom{m}{2}} [x, y, x]^{\binom{m}{3}} [x, y, y]^{\binom{m}{3} - m \binom{m}{2}}, \\ (xy)^m &= x^m y^m [x, y]^{-\binom{m}{2}} [x, y, x]^{-\binom{m}{3}} [x, y, y]^{\binom{m}{3} + (1-m) \binom{m}{2}}, \end{aligned}$$

where $\binom{m}{j} = 0$ if $m < j$.

Proof. These identities can be easily derived from Lemma 7 and 8. \square

Corollary 10. Let G be a nilpotent group of class 3, $x, y \in G$. Then for any nonnegative integers i, j, k, l and m ,

$$\begin{aligned} (x^i y^j)^m &= x^{mi} y^{mj} [x, y]^{-ij \binom{m}{2}} [x, y, x]^{-j \binom{i}{2} \binom{m}{2} - i^2 j \binom{m}{3}} [x, y, y]^{-i \binom{j}{2} \binom{m}{2} + ij^2 \left(\binom{m}{3} + (1-m) \binom{m}{2} \right)}, \\ [x^i y^j, x^k y^l] &= [x, y]^{il - jk} [x, y, x]^{l \binom{i}{2} - j \binom{k}{2}} [x, y, y]^{ijl - kjl + i \binom{l}{2} - k \binom{j}{2}}. \end{aligned}$$

Proof. By Corollary 9, we have

$$\begin{aligned} (x^i y^j)^m &= x^{mi} y^{mj} [x^i, y^j]^{-\binom{m}{2}} [x^i, y^j, x^i]^{-\binom{m}{3}} [x^i, y^j, y^j]^{\binom{m}{3} + (1-m) \binom{m}{2}} \\ &= x^{mi} y^{mj} ([x, y]^{ij} [x, y, x]^{j \binom{i}{2}} [x, y, y]^{i \binom{j}{2}})^{-\binom{m}{2}} \\ &\quad [[x, y]^{ij} [x, y, x]^{j \binom{i}{2}} [x, y, y]^{i \binom{j}{2}}, x^i]^{-\binom{m}{3}} \\ &\quad [[x, y]^{ij} [x, y, x]^{j \binom{i}{2}} [x, y, y]^{i \binom{j}{2}}, y^j]^{\binom{m}{3} + (1-m) \binom{m}{2}} \\ &= x^{mi} y^{mj} [x, y]^{-ij \binom{m}{2}} [x, y, x]^{-j \binom{i}{2} \binom{m}{2}} [x, y, y]^{-i \binom{j}{2} \binom{m}{2}} \\ &\quad [x, y, x]^{-i^2 j \binom{m}{3}} [x, y, y]^{ij^2 \left(\binom{m}{3} + (1-m) \binom{m}{2} \right)} \\ &= x^{mi} y^{mj} [x, y]^{-ij \binom{m}{2}} [x, y, x]^{-j \binom{i}{2} \binom{m}{2} - i^2 j \binom{m}{3}} \\ &\quad [x, y, y]^{-i \binom{j}{2} \binom{m}{2} + ij^2 \left(\binom{m}{3} + (1-m) \binom{m}{2} \right)}. \end{aligned}$$

$$\begin{aligned}
[x^i y^j, x^k y^l] &= [x^i, x^k y^l]^{y^j} [y^j, x^k y^l] \\
&= [x^i, y^l]^{y^j} [y^j, x^k]^{y^l} \\
&= ([x, y]^{il} [x, y, x]^{l \binom{i}{2}} [x, y, y]^{i \binom{l}{2}})^{y^j} ([y, x]^{jk} [y, x, y]^{k \binom{j}{2}} [y, x, x]^{j \binom{k}{2}})^{y^l} \\
&= ([x, y]^{y^j})^{il} ([y, x]^{y^l})^{jk} [x, y, x]^{l \binom{i}{2} - j \binom{k}{2}} [x, y, y]^{i \binom{l}{2} - k \binom{j}{2}} \\
&= ([x, y] [x, y, y^j])^{il} ([y, x] [y, x, y^l])^{jk} [x, y, x]^{l \binom{i}{2} - j \binom{k}{2}} [x, y, y]^{i \binom{l}{2} - k \binom{j}{2}} \\
&= [x, y]^{il - jk} [x, y, x]^{l \binom{i}{2} - j \binom{k}{2}} [x, y, y]^{ijl - kjl + i \binom{l}{2} - k \binom{j}{2}}.
\end{aligned}$$

□

Lemma 11. [13, Chapter III, Theorem 3.15] Let G be a p -group and $\Phi(G)$ the Frattini subgroup of G . If $|G/\Phi(G)| = p^d$, then every minimal generating set of G contains exactly d elements. In particular, $G = \langle x_i \mid i = 1, 2, \dots, d \rangle$ if and only if $G/\Phi(G) = \langle x_i \Phi(G) \mid i = 1, 2, \dots, d \rangle$.

4 Nilpotent totally symmetric dessins of class three

The rest of the paper is devoted to the classification of totally symmetric dessins $D = (G, x, y)$ with a nilpotent automorphism group G of class three. Since each nilpotent group is a direct product of its Sylow subgroups, it suffices to consider the case when G is a p -group of class three. For simplicity such a dessin will be called a *totally symmetric p -dessin of class three*. In this section we give conventions and prove several lemmas.

Let $D = (G, x, y)$ be a totally symmetric p -dessin of class three. Define

$$z = [x, y], \quad u = [z, x] = [x, y, x] \quad \text{and} \quad v = [z, y] = [x, y, y]$$

Since D is totally symmetric, by Eq. (1) each of the following assignments extends to an automorphism of $G \cong F_2/N$:

$$\begin{aligned}
\tau : x &\mapsto y, & y &\mapsto x; \\
\pi : x &\mapsto x^{-1}, & y &\mapsto y; \\
\zeta : x &\mapsto xy, & y &\mapsto y; \\
\iota : x &\mapsto x^{-1}, & y &\mapsto y^{-1}; \\
\xi : x &\mapsto xy^{-1}, & y &\mapsto y.
\end{aligned}$$

where $\iota = \pi\tau\pi\tau$ and $\xi = \zeta^{-1}$.

Lemma 12. *Let (G, x, y) be a totally symmetric p -dessin of class three, and denote $z = [x, y]$, $u = [z, x]$ and $v = [z, y]$. Then under the automorphisms τ , π , ζ , ι and ξ of G the images of z , u and v are summarised in the following table.*

	x	y	z	u	v
τ	y	x	z^{-1}	v^{-1}	u^{-1}
π	x^{-1}	y	$z^{-1}u$	u	v^{-1}
ζ	xy	y	zv	uv	v
ι	x^{-1}	y^{-1}	$zu^{-1}v^{-1}$	u^{-1}	v^{-1}
ξ	xy^{-1}	y	zv^{-1}	uv^{-1}	v

Proof. Since $x^\tau = y$ and $y^\tau = x$, we have

$$\begin{aligned} z^\tau &= [x, y]^\tau = [x^\tau, y^\tau] = [y, x] = z^{-1}, \\ u^\tau &= [z, x]^\tau = [z^\tau, x^\tau] = [z^{-1}, y] = [z, y]^{-1} = v^{-1}, \\ v^\tau &= [z, y]^\tau = [z^\tau, y^\tau] = [z^{-1}, x] = [z, x]^{-1} = u^{-1}. \end{aligned}$$

The proof for other cases is similar and is left to the reader. \square

Now assume that

$$o(x) = p^a, \quad o(z) = p^b \quad \text{and} \quad o(u) = p^c,$$

where a, b, c are nonnegative integers. By Lemma 6, $G_3 = \langle u, v \rangle$ and $G_2 = G' = \langle z, G_3 \rangle$. Define $H = \langle G', x \rangle$. Then $G = \langle H, y \rangle$ and $H \trianglelefteq G$. Assume that

$$\langle x \rangle \cap G' = \langle x^{p^d} \rangle \quad \text{and} \quad \langle y \rangle \cap H = \langle y^{p^e} \rangle$$

where d, e are nonnegative integers. In other words, d and e are the smallest nonnegative integers i and j such that $x^{p^i} \in G'$ and $y^{p^j} \in H$. Note that

$$\langle y \rangle \cap G' = \tau(\langle x \rangle \cap G') = \tau(\langle x^{p^d} \rangle) = \langle \tau(x^{p^d}) \rangle = \langle y^{p^d} \rangle$$

By Lemma 2 $\langle y \rangle \cap H = \langle y \rangle \cap G'$, we have $d = e$. Assume that

$$x^{p^d} = z^l u^m v^n, \tag{6}$$

where l, m, n are nonnegative integers such that $0 \leq l < p^b$ and $0 \leq m, n < p^c$. Then

$$y^{p^d} = \tau(x^{p^d}) = \tau(z^l u^m v^n) = z^{-l} v^{-m} u^{-n}. \tag{7}$$

Lemma 13. *Let (G, x, y) be a totally symmetric p -dessin of class three. Then with the above notation the following statements hold true:*

- (i) $o(y) = o(x)$ and $o(u) = o(v)$;
- (ii) $\langle u \rangle \cap \langle v \rangle = \langle z \rangle \cap G_3 = \langle x \rangle \cap \langle v \rangle = \langle y \rangle \cap \langle u \rangle = 1$;
- (iii) $1 \leq c \leq b \leq d \leq a$;
- (iv) $n = 0$.

Proof. (i) By Lemma 12, the automorphism τ of G transposes x and y , and u and v^{-1} . So $o(y) = o(\tau(y)) = o(x)$ and $o(u) = o(\tau(u)) = o(v^{-1}) = o(v)$.

(ii) Assume that $\langle u \rangle \cap \langle v \rangle = \langle v^h \rangle$. Since $o(u) = o(v)$, we have $u^h = v^{hf}$ for some f coprime to p . Applying the automorphism ζ to the relation we obtain that $\zeta(u^h) = \zeta(v^{hf})$. By Lemma 12 $\zeta(u^h) = \zeta(u)^h = (uv)^h = u^h v^h$ and $\zeta(v^{hf}) = v^{hf} = u^h$. It follows that $u^h v^h = u^h$, and hence $v^h = 1$. This proves that $\langle u \rangle \cap \langle v \rangle = 1$.

Moreover, assume that $\langle z \rangle \cap \langle u, v \rangle = \langle z^k \rangle$. Then $z^k = u^i v^j$ for some integers i and j . Applying τ to the relation we get $\tau(z^k) = \tau(u^i v^j)$. By Lemma 12 we have $\tau(z^k) = \tau(z)^k = z^{-k} = u^{-i} v^{-j}$ and $\tau(u^i v^j) = \tau(u)^i \tau(v)^j = u^{-j} v^{-i}$. It follows that $u^{i-j} = v^{i-j}$. Recall that $o(u) = o(v) = p^c$ and $\langle u \rangle \cap \langle v \rangle = 1$. So we have $i \equiv j \pmod{p^c}$, and hence

$$z^k = u^i v^i.$$

Applying ζ to the relation we get $\zeta(z^k) = \zeta(u^i v^i)$. By Lemma 12 we have $\zeta(z^k) = \zeta(z)^k = (zv)^k = z^k v^k$ and $\zeta(u^i v^i) = \zeta(u)^i \zeta(v)^i = u^i v^{2i}$. So we obtain that $z^k = u^i v^{2i-k}$. Comparing this with previous relation we get $v^{i-k} = 1$. So $i \equiv k \pmod{p^c}$. On the other hand, applying ι to the relation $z^k = u^i v^i$ we deduce that $z^k = u^{k-i} v^{k-i}$. Since $i \equiv k \pmod{p^c}$ and $o(u) = o(v) = p^c$, we obtain that $z^k = 1$. Consequently $\langle z \rangle \cap \langle u, v \rangle = 1$.

Finally, assume that $\langle x \rangle \cap \langle v \rangle = \langle x^i \rangle$ where $i \geq 0$. Then $x^i = v^j$ for some integer j . Applying τ to the relation we have $y^i = \tau(x^i) = \tau(v^j) = u^{-j}$. By Lemma 9 and Lemma 12 we have

$$v^j = \xi(v^j) = \xi(x^i) = (xy^{-1})^i = x^i y^{-i} z^{\binom{i}{2}} u^{\binom{i}{3}} v^{\binom{i}{3}-i\binom{i}{2}} = z^{\binom{i}{2}} u^{j+\binom{i}{3}} v^{j+\binom{i}{3}-i\binom{i}{2}},$$

which is equivalent to

$$z^{-\binom{i}{2}} = u^{j+\binom{i}{3}} v^{\binom{i}{3}-i\binom{i}{2}}.$$

Recall that $\langle u \rangle \cap \langle v \rangle = \langle z \rangle \cap \langle u, v \rangle = 1$, so we have

$$\binom{i}{2} \equiv 0 \pmod{p^b}, \quad (8)$$

$$\binom{i}{3} \equiv -j \pmod{p^c}, \quad (9)$$

$$\binom{i}{3} \equiv i \binom{i}{2} \pmod{p^c}. \quad (10)$$

By induction we deduce that $u^{p^b} = [z, x]^{p^b} = [z^{p^b}, x] = 1$. Recall that $o(u) = p^c$. So we get $c \leq b$. So by (8) we have $\binom{i}{2} \equiv 0 \pmod{p^c}$. Hence (10) is reduced to $\binom{i}{3} \equiv 0 \pmod{p^c}$. Consequently, (9) is reduced to $j \equiv 0 \pmod{p^c}$. Therefore by the assumption $\langle x \rangle \cap \langle v \rangle = 1$. Applying τ we also have $\langle y \rangle \cap \langle u \rangle = \tau(\langle x \rangle \cap \langle v \rangle) = 1$.

(iii) Since G has class 3, $G_4 = 1$ and $G_3 > 1$. Recall that $G_3 = \langle u, v \rangle$ and $o(u) = o(v) = p^c$. So we have $c \geq 1$. In the proof of (ii) we have already shown $c \leq b$. Moreover, by Corollary 9 we have $[x, y^{p^d}] = z^{p^d} v^{\binom{p^d}{2}}$. By (7) we also have

$$[x, y^{p^d}] = [x, z^{-l} v^{-m} u^{-n}] = [x, z^{-l}] = [x, z]^{-l} = u^l.$$

It follows that $z^{p^d} v^{\binom{p^d}{2}} = u^l$, which implies that $z^{p^d} = u^l v^{-\binom{p^d}{2}}$. By Lemma 13, $\langle z \rangle \cap \langle u, v \rangle = \langle u \rangle \cap \langle v \rangle = 1$. So the above relation implies that $z^{p^d} = 1$. Consequently $b \leq d$.

(iv) Applying π to (6) and by Lemma 12 we have

$$x^{-p^d} = \pi(x^{p^d}) = \pi(z^l u^m v^n) = z^{-l} u^{l+m} v^{-n}$$

Combining this with (6) we deduce that $z^{-l} u^{l+m} v^{-n} = z^{-l} u^{-m} v^{-n}$, or equivalently, $u^{l+2m} = 1$. Hence

$$l + 2m \equiv 0 \pmod{p^c}. \quad (11)$$

On the other hand, applying ξ to (6) we have

$$\begin{aligned} z^l u^m v^{-l-m+n} &= \xi(z^l u^m v^n) = \xi(x^{p^d}) = (xy^{-1})^{p^d} \\ &= x^{p^d} y^{-p^d} z^{\binom{p^d}{2}} u^{\binom{p^d}{3}} v^{\binom{p^d}{3} - p^d \binom{p^d}{2}} \\ &= (z^l u^m v^n) (z^l u^n v^m) z^{\binom{p^d}{2}} u^{\binom{p^d}{3}} v^{\binom{p^d}{3} - p^d \binom{p^d}{2}} \\ &= z^{2l + \binom{p^d}{2}} u^{m+n + \binom{p^d}{3}} v^{m+n + \binom{p^d}{3} - p^d \binom{p^d}{2}}. \end{aligned}$$

Hence

$$z^{-l - \binom{p^d}{2}} = u^{n + \binom{p^d}{3}} v^{l + 2m + \binom{p^d}{3} - p^d \binom{p^d}{2}}.$$

By (ii), $\langle z \rangle \cap \langle u, v \rangle = \langle u \rangle \cap \langle v \rangle = 1$. It follows that

$$l + \binom{p^d}{2} \equiv 0 \pmod{p^b}, \quad (12)$$

$$n + \binom{p^d}{3} \equiv 0 \pmod{p^c}, \quad (13)$$

$$l + 2m + \binom{p^d}{3} - p^d \binom{p^d}{2} \equiv 0 \pmod{p^c}. \quad (14)$$

By (iii), $c \leq d$. so $p^d \binom{p^d}{2} \equiv 0 \pmod{p^c}$. Combining this with (11) the congruence (14) is reduced to

$$\binom{p^d}{3} \equiv 0 \pmod{p^c}. \quad (15)$$

Hence (13) is reduced to $n \equiv 0 \pmod{p^c}$. \square

Corollary 14. *The values of numerical parameters l, m, n and a, b, c, d defined above belong to one of the following cases:*

(A) p is odd,

- (i) $p > 3$ and $l = m = n = 0$ and $1 \leq c \leq b \leq d = a$;
- (ii) $p = 3$ and $l = m = n = 0$ and either $1 \leq c < b = d = a$ or $1 \leq c \leq b < d = a$;

(B) $p = 2$,

- (iii) $l = m = n = 0$ and $1 \leq c \leq b < d = a$,
- (iv) $l = n = 0$ and $m = 2^{c-1}$ and $1 \leq c \leq b \leq d - 1 = a - 2$,
- (v) $l = 2^{b-1}$ and $m = n = 0$ and $1 \leq c \leq b - 1$ and $b = d = a - 1$,
- (vi) $l = 2^{b-1}$, $m = q = 2^{c-1}$, $n = 0$ and $1 \leq c \leq b - 1$ and $b = d = a - 1$.

Proof. By Lemma 13(iv), $n = 0$, so Eqs. (6) and (7) are reduced to

$$x^{p^d} = z^l u^m \quad \text{and} \quad y^{p^d} = z^{-l} v^{-m}. \quad (16)$$

Applying ι to the first relation we have

$$z^l u^{-l-m} v^{-l} = \iota(z^l u^m) = \iota(x^{p^d}) = x^{-p^d} = z^{-l} u^{-m},$$

so we obtain $z^{2l} = u^l v^l$. Since $\langle z \rangle \cap \langle u, v \rangle = \langle u \rangle \cap \langle v \rangle = 1$ (see Lemma 13(ii)), we get

$$2l \equiv 0 \pmod{p^b}, \quad (17)$$

$$l \equiv 0 \pmod{p^c}. \quad (18)$$

Combining (18) with (11) we obtain that

$$2m \equiv 0 \pmod{p^c}. \quad (19)$$

Case (A). If p is odd, by (17) and (19) we have $l = m = 0$. Hence by the first relation in (16) we have $x^{p^d} = 1$. Therefore $d = a$. Combining this with Lemma 13(iii) we thus obtain $1 \leq c \leq b \leq d = a$. Eq. (15) motivates us to distinguish two subcases.

Subcase (i). $p > 3$.

In this case, (15) is automatically satisfied.

Subcase (ii). $p = 3$.

Since $3^{d-1} \parallel \binom{p^d}{3}$, by (15), we have $c < d$. So either $1 \leq c < b = d = a$ or $1 \leq c \leq b < d = a$.

Case (B). If $p = 2$, then by (17) and (19) we have one of the following four subcases: (iii) $l = m = 0$; (iv) $l = 0$ and $m = 2^{c-1}$; (v) $l = 2^{b-1}$ and $m = 0$; (vi) $l = 2^{b-1}$ and $m = 2^{c-1}$.

Subcase (iii). $l = m = 0$.

In this case, Eq. (12) is reduced to $\binom{2^d}{2} \equiv 0 \pmod{2^b}$, so $b \leq d - 1$; The first relation in (16) is reduced to $x^{p^d} = 1$, so $d = a$. Combining these the inequality in Lemma 13(iii), we get $1 \leq c \leq b \leq d - 1 = a - 1$.

Subcase (iv). $l = 0$ and $m = 2^{c-1}$.

In this case, Eq. (12) is also reduced to $\binom{2^d}{2} \equiv 0 \pmod{2^b}$, so $b \leq d - 1$; the first relation in (16) is reduced to $x^{p^d} = u^{2^{c-1}}$, so $d = a - 1$. Combining these with the inequalities in Lemma 13(iii)-(iv) we thus obtain $1 \leq c \leq b \leq d - 1 = a - 2$.

Subcase (v). $l = 2^{b-1}$ and $m = 0$.

In this case, Eq. (12) is reduced to $2^{b-1} + \binom{2^d}{2} \equiv 0 \pmod{2^b}$. By (18) we have $2^{b-1} \equiv 0 \pmod{2^c}$. So $c \leq b - 1$ and $b = d$. Note that the first relation in (16) is reduced to $x^{p^d} = z^{2^{b-1}}$, so $d = a - 1$. Combining these with the inequalities in Lemma 13(iii)-(iv) we thus obtain $1 \leq c \leq b = d = a - 1$.

Subcase (vi). $l = 2^{b-1}$ and $m = 2^{c-1}$.

In this case, Eq. (12) is reduced to $2^{b-1} + \binom{2^d}{2} \equiv 0 \pmod{2^b}$. By (18) we have $2^{b-1} \equiv 0 \pmod{2^c}$. So $c \leq b - 1$ and $b = d$. Note that the first relation in (16) is reduced to $x^{p^d} = z^{2^{b-1}} u^{2^{c-1}}$, so $d = a - 1$. Combining these with the inequalities in Lemma 13(iii)-(iv) we thus obtain $1 \leq c \leq b = d = a - 1$.

□

5 Classification

The following theorem is the main result of the paper.

Theorem 15. *Let $D = (G, x, y)$ be a totall symmetric dessin. If G is a p -group of class three, then G is isomorphic to one of the following groups:*

(A) p is odd,

(i) $p > 3$ and $1 \leq c \leq b \leq a$,

$$G = \langle x, y | x^{p^a} = y^{p^a} = z^{p^b} = u^{p^c} = v^{p^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, z := [x, y], u := [z, x], v := [z, y] \rangle.$$

(ii) $p = 3$ and $1 \leq c < b = a$ or $1 \leq c \leq b \leq a - 1$,

$$G = \langle x, y | x^{3^a} = y^{3^a} = z^{3^b} = u^{3^c} = v^{3^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, z := [x, y], u := [z, x], v := [z, y] \rangle.$$

(B) $p = 2$,

(iii) $1 \leq c \leq b \leq a - 1$,

$$G = \langle x, y | x^{2^a} = y^{2^a} = z^{2^b} = u^{2^c} = v^{2^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, z := [x, y], u := [z, x], v := [z, y] \rangle.$$

(iv) $1 \leq c \leq b \leq a - 2$,

$$G = \langle x, y | x^{2^a} = y^{2^a} = z^{2^b} = u^{2^c} = v^{2^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, x^{2^{a-1}} = u^{2^{c-1}}, y^{2^{a-1}} = v^{2^{c-1}}, z := [x, y], u := [z, x], v := [z, y] \rangle.$$

(v) $1 \leq c \leq a - 2$,

$$G = \langle x, y | x^{2^a} = y^{2^a} = z^{2^{a-1}} = u^{2^c} = v^{2^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, x^{2^{a-1}} = z^{2^{a-2}}, y^{2^{a-1}} = z^{2^{a-2}}, z := [x, y], u := [z, x], v := [z, y] \rangle.$$

(vi) $1 \leq c \leq a - 2$,

$$G = \langle x, y | x^{2^a} = y^{2^a} = z^{2^{a-1}} = u^{2^c} = v^{2^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, x^{2^{a-1}} = z^{2^{a-2}} u^{2^{c-1}}, y^{2^{a-1}} = z^{2^{a-2}} v^{2^{c-1}}, z := [x, y], u := [z, x], v := [z, y] \rangle.$$

Moreover, each of the above groups underlies a unique regular dessin, and the groups from distinct families, or from the same family but with distinct parameters, are not isomorphic.

Proof. By the assumption we have $G = \langle x, y \rangle$. Define $z = [x, y]$, $u = [z, x]$ and $v = [z, y]$. Since G is of class three, G is metabelian. So by Lemma 13(i), $o(x) = o(y)$ and $o(u) = o(v)$. Define $o(x) = p^a$, $o(z) = p^b$ and $o(u) = p^c$. By Lemma 6, $G_3 = \langle u, v \rangle$ and $G_2 = \langle z, u, v \rangle$. Let $H = \langle x, z, u, v \rangle$. Then we obtain a series of normal subgroups of G :

$$1 \leq G_3 \leq G_2 \leq H \leq G,$$

where $G_2/G_3 = \langle zG_3 \rangle$, $H/G_2 = \langle xG_2 \rangle$ and $G/H = \langle yH \rangle$ are all cyclic groups. Assume that $\langle x \rangle \cap G_2 = \langle x^{p^d} \rangle$ where d is a nonnegative integer. Then $x^{p^d} = z^l u^m v^n$ where l, m, n are nonnegative integers such that

$$0 \leq l < p^b \quad \text{and} \quad 0 \leq m, n < p^c.$$

By Lemma 2, $\langle y \rangle \cap H = \langle y \rangle \cap G_2$. Since $\langle y \rangle \cap G_2 = \tau(\langle x \rangle \cap G_2)$, we have

$$\langle y \rangle \cap H = \tau(\langle x \rangle \cap G_2) = \tau(\langle x^{p^d} \rangle) = \langle y^{p^d} \rangle.$$

We have $y^{p^d} = \tau(x^{p^d}) = \tau(z^l u^m v^n) = z^{-l} v^{-m} u^{-n}$. By Lemma 13(iv), $n = 0$. Therefore, by Lemma 13(ii) the group G has a presentation

$$G = \langle x, y \mid x^{p^a} = y^{p^a} = z^{p^b} = u^{p^c} = v^{p^c} = [x, u] = [x, v] = [y, u] = [y, v] = 1, \\ x^{p^d} = z^l u^m, y^{p^d} = z^{-l} v^{-m}, z := [x, y], u := [z, x], v := [z, y] \rangle,$$

By filling the numerical conditions proved in Corollary 14 the presentation is simplified to the stated forms.

To show that the group G underlies a unique regular dessin, by Proposition 3(ii) it is sufficient to show that $\text{Aut}(G)$ is transitive on the generating pairs of G . By Burnside's Basis Theorem each generating pair (x_1, y_1) of G can be written as the form

$$(x_1, y_1) = (x^{i_1} y^{i_2} z^{i_3} u^{i_4} v^{i_5}, x^{j_1} y^{j_2} z^{j_3} u^{j_4} v^{j_5})$$

where

$$i_1 j_2 - i_2 j_1 \not\equiv 0 \pmod{p}. \quad (20)$$

So it suffices to verify that the assignment $x \mapsto x_1, y \mapsto y_1$ extends to a group automorphism of G . Define $z_1 = [x_1, y_1]$, $u_1 = [z_1, x_1]$ and $v_1 = [z_1, y_1]$. Then

$$\begin{aligned}
z_1 &= [x_1, y_1] = [x^{i_1} y^{i_2} z^{i_3} u^{i_4} v^{i_5}, x^{j_1} y^{j_2} z^{j_3} u^{j_4} v^{j_5}] \\
&= [x^{i_1} y^{i_2} z^{i_3}, x^{j_1} y^{j_2} z^{j_3}] \\
&= [x^{i_1} y^{i_2}, x^{j_1} y^{j_2} z^{j_3}] [z^{i_3}, x^{j_1} y^{j_2} z^{j_3}] \\
&= [x^{i_1} y^{i_2}, x^{j_1} y^{j_2}] [x^{i_1} y^{i_2}, z^{j_3}] [z^{i_3}, x^{j_1} y^{j_2}] \\
&= z^{i_1 j_2 - i_2 j_1} u^{j_2 \binom{i_1}{2} - i_2 \binom{j_1}{2}} v^{i_1 i_2 j_2 - j_1 i_2 j_2 + i_1 \binom{j_2}{2} - j_1 \binom{i_2}{2}} \\
&\quad [x^{i_1}, z^{j_3}] [y^{i_2}, z^{j_3}] [z^{i_3}, y^{j_2}] [z^{i_3}, x^{j_1}] \\
&= z^L u^M v^N,
\end{aligned}$$

where

$$L = i_1 j_2 - i_2 j_1, \quad (21)$$

$$M = j_2 \binom{i_1}{2} - i_2 \binom{j_1}{2} - i_1 j_3 + i_3 j_1, \quad (22)$$

$$N = i_1 i_2 j_2 - j_1 i_2 j_2 + i_1 \binom{j_2}{2} - j_1 \binom{i_2}{2} - i_2 j_3 + i_3 j_2. \quad (23)$$

We also have

$$\begin{aligned}
u_1 &= [z_1, x_1] = [z^L u^M v^N, x^{i_1} y^{i_2} z^{i_3} u^{i_4} v^{i_5}] = [z^L, x^{i_1} y^{i_2} z^{i_3}] \\
&= [z^L, x^{i_1} y^{i_2}] = [z^L, y^{i_2}] [z^L, x^{i_1}] = u^{L i_1} v^{L i_2},
\end{aligned}$$

and

$$\begin{aligned}
v_1 &:= [z_1, y_1] = [z^L u^M v^N, x^{j_1} y^{j_2} z^{j_3} u^{j_4} v^{j_5}] = [z^L, x^{j_1} y^{j_2} z^{j_3}] \\
&= [z^L, x^{j_1} y^{j_2}] = [z^L, y^{j_2}] [z^L, x^{j_1}] = u^{L j_1} v^{L j_2}.
\end{aligned}$$

Clearly, in each case

$$z_1^{p^b} = u_1^{p^c} = v_1^{p^c} = [x_1, u_1] = [x_1, v_1] = [y_1, u_1] = [y_1, v_1] = 1.$$

In what follows we verify that x_1 and y_1 fulfil the remaining defining relations case by case.

Case (i). $p > 3, 1 \leq c \leq b \leq d = a$.

In this case we need to show that $x_1^{p^a} = 1$ and $y_1^{p^a} = 1$. By Corollary 9 and Corollary 10 we have

$$\begin{aligned}
x_1^{p^a} &= (x^{i_1} y^{i_2} z^{i_3} u^{i_4} v^{i_5})^{p^a} = ((x^{i_1} y^{i_2}) z^{i_3})^{p^a} u^{i_4 p^a} v^{i_5 p^a} \\
&= (x^{i_1} y^{i_2})^{p^a} z^{i_3 p^a} [x^{i_1} y^{i_2}, z]^{-i_3 \binom{p^a}{2}} u^{i_4 p^a} v^{i_5 p^a} \\
&= x^{i_1 p^a} y^{i_2 p^a} z^R u^S v^T = z^R u^S v^T,
\end{aligned}$$

where

$$R = i_3 p^a - i_1 i_2 \binom{p^a}{2}, \quad (24)$$

$$S = -i_2 \binom{i_1}{2} \binom{p^a}{2} - i_1^2 i_2 \binom{p^a}{3} + i_1 i_3 \binom{p^a}{2} + i_4 p^a, \quad (25)$$

$$T = -i_1 \binom{i_2}{2} \binom{p^a}{2} + i_1 i_2^2 \left(\binom{p^a}{3} + (1 - p^a) \binom{p^a}{2} \right) + i_2 i_3 \binom{p^a}{2} + i_5 p^a. \quad (26)$$

Recall that $p > 3$ is odd, so $p^a | \binom{p^a}{2}$ and $p^a | \binom{p^a}{3}$. So $p^a | R$, $p^a | S$ and $p^a | T$, and hence $x_1^{p^a} = 1$. Similarly, $y_1^{p^a} = 1$.

Case (ii). $p = 3$ and $1 \leq c < b = d = a$ or $1 \leq c \leq b < e = d = a$.

Note that $3^a | \binom{3^a}{2}$ and $3^{a-1} | \binom{3^a}{3}$. Using similar arguments as in (i) it is straightforward to verify that $x_1^{3^a} = 1$ and $y_1^{3^a} = 1$.

Case (iii). $p = 2$ and $1 \leq c \leq b \leq d - 1 = a - 1$.

Note that $2^{a-1} | \binom{2^a}{2}$ and $2^a | \binom{2^a}{3}$. Using similar arguments as in (i) it is straightforward to verify that $x_1^{2^a} = 1$ and $y_1^{2^a} = 1$.

Case (iv). $p = 2$ and $1 \leq c \leq b \leq e - 1 = a - 2$.

Using similar arguments as in (i) it is easy to prove that $x_1^{2^a} = y_1^{2^a} = 1$. Since $2^{a-2} | \binom{2^{a-1}}{2}$ and $2^{a-1} | \binom{2^{a-1}}{3}$, we have

$$x_1^{2^{a-1}} = x^{i_1 2^{a-1}} y^{i_2 2^{a-1}} = u^{i_1 2^{c-1}} v^{i_2 2^{c-1}}$$

and

$$u_1^{2^{c-1}} = u^{Li_1 2^{c-1}} v^{Li_2 2^{c-1}} = u^{i_1 2^{c-1}} v^{i_2 2^{c-1}}.$$

So $x_1^{2^{a-1}} = u_1^{2^{c-1}}$. Similarly, $y_1^{2^{a-1}} = v_1^{2^{c-1}}$.

Case (v). $p = 2$ and $1 \leq c \leq b - 1 = d - 1 = a - 2$.

Using similar arguments as in (i) it is easy to prove that $x_1^{2^a} = y_1^{2^a} = 1$. Since $2^{a-2} | \binom{2^{a-1}}{2}$ and $2^{a-1} | \binom{2^{a-1}}{3}$, we have

$$\begin{aligned} x_1^{2^{a-1}} &= x^{i_1 2^{a-1}} y^{i_2 2^{a-1}} z^{-i_1 i_2 2^{a-2} (2^{a-1} - 1)} \\ &= z^{(i_1 + i_2 - i_1 i_2 (2^{a-1} - 1)) 2^{a-2}} = z^{2^{a-2}} \end{aligned}$$

and

$$z_1^{2^{a-2}} = z^{(i_1 j_2 - i_2 j_1) 2^{a-2}} = z^{2^{a-2}}.$$

Hence $x_1^{2^{a-1}} = z_1^{2^{a-2}}$. Similarly, $y_1^{2^{a-1}} = z_1^{2^{a-2}}$.

Case (vi). $p = 2$ and $1 \leq c \leq b - 1 = d - 1 = a - 2$.

Using similar arguments as in (i) it is easy to prove that $x_1^{2^a} = y_1^{2^a} = 1$. Since $2^{a-2} \mid \binom{2^{a-1}}{2}$ and $2^{a-1} \mid \binom{2^{a-1}}{3}$, we have

$$\begin{aligned} x_1^{2^{a-1}} &= x^{i_1 2^{a-1}} y^{i_2 2^{a-1}} z^{-i_1 i_2 2^{a-2} (2^{a-1} - 1)} = z^{(i_1 + i_2 - i_1 i_2 (2^{a-1} - 1)) 2^{a-2}} u^{i_1 2^{c-1}} v^{i_2 2^{c-1}} \\ &= z^{2^{a-2}} u^{i_1 2^{c-1}} v^{i_2 2^{c-1}} \end{aligned}$$

and

$$z_1^{2^{a-2}} u_1^{2^{c-1}} = z^{(i_1 j_2 - i_2 j_1) 2^{a-2}} u^{Li_1 2^{c-1}} v^{Li_2 2^{c-1}} = z^{2^{a-2}} u^{i_1 2^{c-1}} v^{i_2 2^{c-1}}.$$

Hence $x_1^{2^{a-1}} = z_1^{2^{a-2}} u_1^{2^{c-1}}$. Similarly, $y_1^{2^{a-1}} = z_1^{2^{a-2}} v_1^{2^{c-1}}$.

Finally, to prove the isomorphism relations between the groups we summarize the invariant types of G' and $G^{\text{ab}} = G/G'$ as follows.

Case	G'	G^{ab}	Condition
(i)	$C_{p^c} \times C_{p^c} \times C_{p^b}$	$C_{p^a} \times C_{p^a}$	$1 \leq c \leq b \leq a$
(ii)	$C_{3^c} \times C_{3^c} \times C_{3^b}$	$C_{3^a} \times C_{3^a}$	$1 \leq c < b \leq a$ or $1 \leq c \leq b \leq a - 1$
(iii)	$C_{2^c} \times C_{2^c} \times C_{2^b}$	$C_{2^a} \times C_{2^a}$	$1 \leq c \leq b \leq a - 1$
(iv)	$C_{2^c} \times C_{2^c} \times C_{2^b}$	$C_{2^{a-1}} \times C_{2^{a-1}}$	$1 \leq c \leq b \leq a - 2$
(v)	$C_{2^c} \times C_{2^c} \times C_{2^{a-1}}$	$C_{2^{a-1}} \times C_{2^{a-1}}$	$1 \leq c \leq a - 2$
(vi)	$C_{2^c} \times C_{2^c} \times C_{2^{a-1}}$	$C_{2^{a-1}} \times C_{2^{a-1}}$	$1 \leq c \leq a - 2$

It is clear that the groups are pairwise non-isomorphic, except possibly the groups from (v) and (vi). But each of the groups has a unique presentation, so by comparing the presentations we find that every group from (v) is not isomorphic to any group from (vi), as claimed. \square

Corollary 16. *Let G be a group from Theorem 15. Then the size of the group G and its automorphism group $\text{Aut}(G)$, and the type and genus of the associated totally symmetric dessin D with $\text{Aut}(D) \cong G$ are summarized as follows.*

G	$ G $	$ \text{Aut}(G) $	Type of D	Genus of D
(i)	$p^{2(a+c)+b}$	$p^{4a+2b+4c-3}(p+1)(p-1)^2$	(p^a, p^a, p^a)	$p^{a+b+2c}(p^a - 3)/2 + 1$
(ii)	$3^{2(a+c)+b}$	$2^4 \cdot 3^{4a+2b+4c-3}$	$(3^a, 3^a, 3^a)$	$3^{a+b+2c+1}(3^{a-1} - 1)/2 + 1$
(iii)	$2^{2(a+c)+b}$	$3 \cdot 2^{4a+2b+4c-3}$	$(2^a, 2^a, 2^a)$	$2^{a+b+2c-1}(2^a - 3) + 1$
(iv)	$2^{2(a+c)+b-2}$	$3 \cdot 2^{4a+2b+4c-7}$	$(2^a, 2^a, 2^a)$	$2^{a+b+2c-3}(2^a - 3) + 1$
(v)	$2^{3a+2c-3}$	$3 \cdot 2^{6a+4c-9}$	$(2^a, 2^a, 2^a)$	$2^{2a+2c-4}(2^a - 3) + 1$
(vi)	$2^{3a+2c-3}$	$3 \cdot 2^{6a+4c-9}$	$(2^a, 2^a, 2^a)$	$2^{2a+2c-4}(2^a - 3) + 1$

Remark 1. In [2, Research problems and themes I 35(a)], Berkovich and Janko posed a problem of studying p -group G with $|G : \Phi(G)| = p^d$ satisfying

$$|\mathrm{Aut}(G)| = (p^d - 1)(p^d - p) \dots (p^d - p^{d-1})|\Phi(G)|^d,$$

that is, G is a d -generator p -group whose automorphism group $\mathrm{Aut}(G)$ acts transitively on its generating d -tuples. Theorem 15 and Corollary 16 is an answer to this problem for $d = 2$ and $c(G) = 3$.

Acknowledgement

The first and third author were supported by Zhejiang Provincial Natural Science Foundation of China under Grant No. LY16A010010, and by Scientific Research Foundation(SRF) of Zhejiang Ocean University (21065014015, 21065014115). The second author was supported by the following grants: VEGA 1/0150/14, APVV-0223-10, and the grant APVV-ESF-EC-0009-10 within the EUROCORES Programme EUROGIGA (Project GReGAS) of the European Science Foundation and the Slovak-Chinese bilateral grant APVV-SK-CN-0009-12.

References

- [1] G.V. Belyĭ, Galois extensions of a maximal cyclotomic field, *Izv. Akad. Nauk. SSSR Ser. Mat.* 43 (1979) 267–276
- [2] Y. Berkovich, Z. Janko, *Groups of Prime Power Order (Vol I)*, Walter de Gruyter & Co, 2008
- [3] A. Breda d’Azevedo, G.A. Jones, Platonic hypermaps, *Contributions to Algebra and Geometry* 42(1) (2001) 1–37
- [4] M.D.E. Conder, S.-F. Du, R. Nedela, M. Škovič, Bounding the size of a regular map with nilpotent automorphism group, in preparation.
- [5] M.D.E. Conder, G.A. Jones, M. Streit, J. Wolfart, Galois actions and regular dessins of small genera, *Rev. Mat. Iberoam.* 29 (2013) 163–181
- [6] D. Corn, D. Singerman, Regular hypermaps, *European J. Combin.* 9 (1988) 337–351
- [7] A.D. Coste, G.A. Jones, M. Streit, J. Wolfart, Generalised Fermat hypermaps and Galois orbits, *Glasgow Math. J.* 51 (2) (2009) 289–299

- [8] S.F. Du, et al, Regular embeddings of $K_{n,n}$ where n is a power of 2. I: Metacyclic case, *European Journal of Combinatorics* 28(6) (2007) 1595–1609
- [9] G. González-Diez, A. Jaikin-Zapirain, The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces, preprint, 2013
- [10] A. Grothendieck, Esquisse d’un programme, in: L. Schneps and P. Lochak (eds.), *Geometric Galois actions 1. The inverse Galois problem, Moduli Spaces and Mapping Class Groups*, London Math. Soc. Lecture Notes Ser. 242, pp. 5–48, Cambridge Univ. Press, Cambridge, 1997
- [11] K. Hu, R. Nedela, N.-E Wang, Nilpotent dessins: Decomposition theorem and classification of the abelian dessins, preprint.
- [12] K. Hu, R. Nedela, N.-E. Wang, Nilpotent groups of class two which underly a unique regular dessin, *Geom. Dedicata*, DOI 10.1007/S10711-015-0074-8
- [13] B. Huppert, *Endliche Gruppen* (Vol. 1), Springer-Verlag, Berlin, 1967
- [14] G.A. Jones, Regular embeddings of complete bipartite graphs: classification and enumeration, *Proc. Lond. Math. Soc.* 101 (3) (2010) 427–453
- [15] G.A. Jones, Regular dessins with a given automorphism group. In: Izquierdo, M., Broughton, S.A., Costa, A.F., Rodríguez, R.E., (eds) *Riemann and Klein surfaces, Automorphisms, Symmetries and Moduli Spaces*. American Math. Soc., Providence, Rhode Island (2014)
- [16] G.A. Jones, D. Pinto, Hypermap operations of finite order, *Discrete Math.* 310 (2010) 1820–1827
- [17] G.A. Jones, D. Singerman, Belyĭ functions, hypermaps and Galois groups, *Bull. London Math. Soc.* 28 (1996) 561–590
- [18] G.A. Jones, M. Streit, J. Wolfart, Galois action on families of generalised Fermat curves, *J. Algebra*, 307 (2007) 829–840
- [19] G.A. Jones, M. Streit, J. Wolfart, Wilson’s map operations on regular dessins and cyclotomic fields of definition, *Proceedings of the London Math. Soc.* 100 (2) (2010) 510–532
- [20] A. Malnič, R. Nedela, M. Škoviera, Regular maps with nilpotent automorphism groups, *European J. Combin.* 33 (8) (2012) 1974–1986

- [21] L. Schneps, Dessins d'enfants on the Riemann sphere, in The Grothendieck Theory of Dessins d'Enfants (Luminy, 1993), 47–77, London Math. Soc. Lecture Note Ser. 200, Cambridge Univ. Press, 1994
- [22] J. Siran, How symmetric can maps on surfaces be? in: Surveys in combinatorics 2013, London Math. Soc. Lecture Note Ser. 409, Cambridge Univ. Press, Cambridge, 2013, 161-238
- [23] M.-Y. Xu, H.-P. Qu, Finite p -Groups, Peking University Press, Beijing, 2010